INDIANA STATE POLICE IDACS SECTION
                         LESSON PLAN

LECTURE:            AREAS OF LIABILITY COURSE
INSTRUCTOR:
SUBJECT MATTER        REMARKS                          (STUDENT USE)

                   IDACS AREAS OF LIABILITY


I.   Introduction

     Administrators have the responsibility of
     directing all areas within their agency. The
     improper use of IDACS/NCIC/NLETS System Data
     has become an important area of concern, not
     only for IDACS and NCIC officials, but for
     local agencies as well. This seminar is
     designed to increase the awareness of the
     problems that can occur in using system data,
     and what can be done to help minimize the risk
     of liability.

     NCIC tracks litigation around the country
     concerning the maintenance and dissemination
     of criminal justice data and publishes items
     of interest in a pamphlet entitled "Areas Of
     Liability for the criminal Justice Information
     System Administrator" which will be used
     during this seminar and is suggested reading.


II.  Objectives

     At the completion of this lecture,
     departmental administrators and upper level
     management personnel will be able to orally
     explain many important areas where their
     agency can become more effective in managing
     IDACS/NCIC/NLETS system data.

---------------------------------------------


III. Awareness Of The Problem

     There have been many documented civil law
     suits for improper use of system data. The
     following are a few of the more famous cases
     from which valuable lessons can be learned.

     A.

        1.   Sheila Jackson-Stossier was arrested/
             detained in New Orleans, based solely
             on an NCIC hit in which a Sheila
             Jackson (similar name) was wanted for
             parole violation in Houston. She was
             detained six (6) days before release.

a. Arresting officer/agency did not compare descriptive data from the hit with her physical description (there were many differences).

b. Arresting officer/agency did not attempt to confirm the hit with the originating agency before arrest and detention.

2. A law suit resulted in a judgement against the arresting officer/agency.

3. To avoid this kind of' liability, follow established guidelines:

a. Operators/Officers should be trained to compare descriptive data on "hits" with person being detained, and

b. operators/officers should confirm "hits" before taking any enforcement action.

1) "hits" are lead information only!

4. Also see Indiana 240 IAC 5-1-1, ... restrictions on use:

... The IDACS provides information for decision making, by investigators and patrolmen. The information furnished through IDACS shall be evaluated with other facts known to the officer and investigators at the scene. IDACS is an information tool. It is no substitute for professional police judgment.

When an agency receives a positive response (wanted notice) from IDACS or NCIC, if the request is urgent, a "U" will be shown in the Priority Field, an immediate follow-up confirmation request with the agency that originated the record in the system is necessary before any enforcement action is taken. Likewise, the originating agency has an obligation to supply a substantive response within 10 minutes to the inquiring agency. However, if the request is routine, a "R" will be shown in the Priority Field, and the response time is up

to one (1) hour. Both of these
responses shall include a
confirmation or denial of the
wanted notice, or the length of
time it will take to respond...

B.   Walcowski v. Macomb County & the State


1.   Walcowski was stopped on a broken
     tail light violation and arrested
     based on an NCIC wanted person hit
     that was in file with the wrong
     charge (purgery, which is a felony).
     Subject was actually wanted for
     contempt of court (a misdemeanor).

2.   Subject sued for battery, assault,
     false arrest, unlawful
     imprisonment, and defamation. In
     the same action, the subject sued
     the director of the Michigan State
     System.

3.   The court ruled that the State
     was immune from this liability,
     because the entering agency is
     responsible for the records in file
     and not the overseeing agency.

4.   To avoid this kind of liability:

     a.   Quality control procedures
          should be implemented by your
          agency which includes a third
          party checking procedure.

     b.   Established validation
          procedures should more closely
          be followed.

5.   Also see Indiana 240 IAC 5-2-9...
     Quality Assurance...

     User Agency agrees to abide by
     accepted quality assurance methods.
     This includes compliance with
     validation procedures as specified
     in the Indiana Administrative Code,
     NCIC serious error procedures, and
     IDACS Quality Control procedures.

     User Agency further agrees to
     establish local procedures whereby
     updates to the wanted files are
     reviewed for accuracy by comparing
     the update with supporting

documentation. This comparison shall
be made by a person other than the
operator who accomplished the update
and the investigating officer who
ordered it.

and Indiana 240 IAC 5-2-7,
Validation of records:

All IDACS user agencies shall
validate, on a periodic basis,
all IDACS and NCIC wanted
records entered on their
authority. Validation of
records shall be in
conformity and compliance with
guidelines set forth by IDACS
and NCIC.

Validation (according to
current NCICI/IDACS policy)
obligates the originating
agency to confirm the record
is COMPLETE, ACCURATE and is
still OUTSTANDING or ACTIVE.

Validation is accomplished by
reviewing the original entry
and current supporting
documents and by recent
consultation with any
appropriate complainant,
victim, prosecutor, court,
motor vehicle registry files
or other appropriate source
or individual. In the event
the originating agency is
unsuccessful in its attempts
to contact the victim,
complainant, etc., the
entering authority shall make
a determination based on the
best information and
knowledge available whether
or not to retain the original
entry on file.

C.  Maney v. Ratcliff

    1.  Subject was arrested on three
        (3) separate occasions based
        on an NCIC hit indicating that
        he was wanted by authorities
        on a felony narcotics charge,
        and each time was not
        extradited, and entry not
        removed.

2. Court ruled that failure to take the entry out of NCIC "evinced a reckless and careless disregard for the subject's constitutional rights."

4. To avoid this kind of liability procedures should be adopted that would more timely identify invalid warrants in order to remove them from file.

5. Also see Indiana 240 IAC 5-1-1, ... restrictions on use.

   Accuracy is essential as is promptness in entering, modifying, locating, or clearing records in the system. Each record on file is identified with the agency originating that record and that agency alone is responsible for the accuracy, completeness, and correct status of that record at all times.

D.  Terry Dean Rogan v City of Los Angeles

   1. Rogan sued the city and two police officers for constantly being arrested and released based on an erroneous NCIC entry made by the officers.

      a.  Officers continually re-entered an NCIC entry even though the data was in error.

   2. The court held that the officers were not liable because they had not been trained on how to change data within the NCIC record and that the City was liable because they made no effort to train officers in proper use of the system.

   3. To avoid this kind of liability training should be given to all personnel in the proper operation of the system (not just operators/coordinators).

4. Also see Indiana 240 IAC 5-2-8, Terminal Agency Operation....

   Agency Operation- Internal. Once operational on the IDACS System, each terminal agency is required to designate one individual as coordinator to serve as liaison between that department and the IDACS Committee. It is important that the person selected becomes familiar with all phases of IDACS to efficiently carry out all duties and responsibilities assigned. Duties and responsibilities are to:

   Insure that all agency personnel (including any non-terminal agencies serviced) utilizing system information are aware of the rules and policies of the IDACS/NCIC/NLETS System...

   and Indiana 240 IAC 5-2-11 IDACS Training.

   Insure that terminal operators receive proper training in accordance with the IDACS Certification Training Program.

   All IDACS Terminal operators (including mobile terminals) shall be trained and tested for their proficiency at operating the IDACS terminal. All IDACS Coordinators shall be trained and tested for their proficiency at operating the IDACS terminal and for their skills as the coordinator.

   To insure that terminal operators and coordinators are familiar with the laws governing IDACS/NCIC/NLETS, System rules, regulations, and procedures, and what files (functions) are available and how to utilize them properly.

   Create an awareness of IDACS/NCIC/NLETS System capabilities in order to allow criminal justice agencies to obtain maximum use of the system.

All persons assigned a system
password (Operator Identifier) to
operate the IDACS terminal and
persons designated IDACS Coordinator
by their agency shall be trained and
tested according to the guidelines
set forth by the IDACS Committee and
approved by the State Police
Superintendent.

The IDACS Committee can authorize
the removal of a system password(s),
or impose sanctions on an agency for
non-compliance with these procedures...

------------------------------------------------

IV.   Solutions and Tools To Minimize Risk

    A.   Operating Procedures

        1.   Local agencies should also have
            written departmental procedures
            which instruct employees to follow
            IDACS/NCIC rules, regulations, and
            procedures.

        2.   Use IDACS/NCIC Operating Manuals,
            and NCIC Code Manual.

    B.  Keep aware of needs and problems
       through IDACS Coordinator.

       Follow Indiana 240 IAC 5-2-8,
       Terminal Agency Operation....

           Agency Operation-Internal. Once
           operational on the IDACS System,
           each terminal agency is required
           to designate one individual as
           coordinator to serve as liaison
           between that department and the
           IDACS Committee. It is important
           that the person selected becomes
           familiar with all phases of IDACS
           to efficiently carry out all
           duties and responsibilities
           assigned. Duties and
           responsibilities are to:

           Insure that all agency personnel
           (including any non-terminal
           agencies serviced) utilizing
           system information are aware of
           the rules and policies of the
           IDACS/NCIC/NLETS System...

C.  Follow Indiana 240 IAC 5-2-11,
    ...Training...

        Sec. 11. All IDACS Terminal
        Operators (including mobile
        terminals) shall be trained and
        tested for their proficiency at
        operating the IDACS terminal. All
        IDACS Coordinators shall be
        trained and tested for their
        proficiency at operating the IDACS
        terminal and for their skills as
        the coordinator.

        (1) All persons assigned a system
        password (operator Identifier) to
        operate the IDACS terminal and
        persons designated IDACS
        Coordinator by their agency shall
        be trained and tested according
        to the guidelines set forth by
        the IDACS Committee and approved
        by State Police Superintendent.

    1.  New operators must be certified
        within the first six months, and
        re-certified every two years
        thereafter.

    2.  New coordinators must be a
        certified operator and certified
        as a coordinator within six
        months after the appointment, and
        re-certified every two years
        thereafter.

    3.  Seminars are available for users
        of the system (records personnel,
        officers, administrators,
        probation officers, prosecutors,
        judges).

        a.  What is available on the
            system, rules for use of the
            data.

    4.  Seminars are available for
        administrators concerning
        liabilities that can occur in
        misuse of system data.

D.  Follow Indiana 240 IAC 5-2-10
    Security; confidentiality...

        SYSTEM as used in the Security
        and Confidentiality Rules shall
        mean IDACS, NLETS, and/or NCIC

terminals, equipment and any
and all data accessible from or
stored therein.

(b) Who May Access SYSTEM Data.
(1) Access, meaning the ability
to obtain information from the
System, shall be permitted only
to criminal justice agencies in
the discharge of their official
mandated responsibilities, and
those agencies as required by
state and/or federal enabling
authority. Release of Indiana
BMV data to non-criminal justice
agencies may occur when it is
determined to be in the best
interest of law enforcement/
criminal justice to do so.
Agencies that shall be
permitted access to SYSTEM data
include:

(A) Police forces and departments
at all governmental levels
(including private college and
railroad police departments as
authorized by Indiana Code) that
are responsible for enforcement
of general criminal laws.

(B) Prosecutive agencies and
departments at all governmental
levels.

(C) Courts at all governmental
levels with a criminal or
equivalent jurisdiction.

(D) Correction departments at all
governmental levels, including
corrective institutions and
probation departments.

(E) Parole commissions and
agencies at all governmental
levels.

(F) Agencies at all governmental
levels which have as a principal
function the collection and
provision of fingerprint
identification information.

(G) Regional or local
governmental organizations
established pursuant to

statute which collect and
process criminal justice
information and whose policy
and governing boards have, as
a minimum, a majority
composition of members
representing criminal justice
agencies.

(2) Limited access. Approved
non-criminal justice agencies
may have access to SYSTEM data
on a limited basis. Limited
basis shall mean restricted to
only that data recommended
through resolution by the IDACS
Committee and approved by the
State Police Superintendent.

E.  Follow Indiana Code 5-2-5-12 Indiana
    Data and Communications System;
    entry of information in computer.

On a daily basis, all law
enforcement agencies shall enter
into the Indiana Data and
Communications (IDACS) computer
the following:

(1) All information concerning
any stolen or recovered property,
including motor vehicles, firearms,
securities, boats, license plates,
and any other stolen or recovered
property.

(2) All information concerning
fugitives charged with any crime,
including information concerning
extradition.

(3) All information concerning
runaways and missing persons,
including information concerning
the release of such persons to the
custody of a parent or guardian.

F.  Follow Indiana 240 IAC 5-2-9 IDACS/
    NCIC hit confirmation procedures...

User Agency agrees to insure that
hit confirmation is available 24
hours a day on records entered
into the wanted files. This
includes being able to provide a
substantive response to an inquiry
within 10 minutes...

1) Upon receipt of a hit
confirmation request, the
originating agency must within ten
minutes furnish a substantive
response, i.e., a positive or
negative confirmation or notice of
the time it will take to confirm
or reject.

2) If no response is received by
the requesting agency within ten
minutes, send a second request.

3) If no response is received from
the second request, send a third
message and this time include the
SP Data Operations Center, the
State Control Terminal of the
originating agency, and FBI NCIC.
No action will be taken by NCIC,
unless the two control terminal
agencies cannot resolve the matter.

a.  Verify warrants, review cases,
and contact complainants to
proper confirm hits.

G.  Follow Indiana 240 IAC 5-2-7,
Validation of Records...

1.  Validation Definition:

(1) Validation (according to
current NCIC/IDACS policy)
obligates the originating agency
to confirm the record is COMPLETE,
ACCURATE and is still OUTSTANDING
or ACTIVE.

(2) Validation is accomplished by
reviewing the original entry and
current supporting documents and
by recent consultation with any
appropriate complainant, victim,
prosecutor, court, motor vehicle
registry files or other
appropriate source or individual.
In the event the originating
agency is unsuccessful in its
attempts to contact the victim,
complainant, etc., the entering
authority shall make a
determination based on the best
information and knowledge
available whether or not to
retain the original entry on file.

2.  Objectives of Validation
    Requirements

    (1) To insure the validity of
    IDACS and NCIC records,
    administrative controls shall be
    maintained which will result in
    prompt updating for the benefit
    of system users.

    (A) Agencies entering records in
    IDACS and/or NCIC are solely
    responsible for their accuracy,
    timeliness, and completeness.

    (B) Only by conscientious
    validation of records can users
    remain assured the integrity of
    the system is being upheld, and
    inquiring officers can rely on
    the information in IDACS and NCIC.

3.  on-line validation transaction
    must be completed.

    a.  Records not validated will
        be purged.

    b.  Records not active should be
        deleted from file by
        entering agency.

    c.  A record left in the system,
        or a record that should have
        been validated and is purged
        could cause risk of
        liability to the originating
        agency if harm occurs to a
        third party due to this
        negligent act.

H.  Follow Indiana 240 IAC 5-2-9,
    ...Quality Assurance...

    User Agency agrees to abide by
    accepted quality assurance methods.
    This includes compliance with
    validation procedures as specified
    in the Indiana Administrative Code,
    NCIC serious error procedures, and
    IDACS Quality Control procedures.

    User Agency further agrees to
    establish local procedures whereby
    updates to the wanted files are
    reviewed for accuracy by comparing

the update with supporting
documentation. This comparison
shall be made by a person other
than the operator who accomplished
the update and the investigating
officer who ordered it.

1.  The following is a list of NCIC
    serious errors which when
    discovered are canceled by NCIC.

    a.  Wanted Person records which
        have an appended locate
        indicating the subject will
        be extradited.

    b.  Wanted Person records
        indicating the subject is
        wanted for questioning only.

    c.  Wanted Person records
        entered for missing persons.

    d.  Security File records that
        do not meet criteria in the
        type field (personal checks,
        cashiers checks, etc.).

    e.  Records entered for stolen
        credit cards.

    f.  Wanted Person records which
        have a MIS field statement
        indicating the individual
        will not be extradited, or
        extradited this state only.

    g.  Wanted Person record that
        has extradition limitations
        and the entering agency has
        not indicated as such in the
        MIS field.

    h.  A wanted file record
        containing inaccurate BMV or
        vehicular data which has been
        verified by a states motor
        vehicles files.

    i.  Records entered in the wrong
        file.

    j.  Property records allowed to
        remain in file in excess of
        ten days after the date of
        locate.

k.  Property records entered with
       non-unique serial numbers,
       owner applied number in the
       SER field, etc.

   l.  Property records entered with
       generic Brand or Make codes
       for which there is no further
       description in the MIS field.

2.  IDACS Quality Control Measures
    identify errors which could cause
    a missed hit, etc.

    a.  Review of daily logs.

        1)  CHRI log
        2)  Wanted File update log
        3)  Switched message log

3.  Agency notified of error and
    asked correct immediately or
    cancel record.

I.  Follow Indiana 240 IAC 5-2-9, User
    Agreements

        All IDACS user agencies shall
        complete a "User Agreement"
        before utilizing the system.
        Agencies with terminals and
        Statutory Police agencies
        shall complete such agreements
        with the Indiana State Police
        and the IDACS Committee. Non-
        terminal agencies shall
        complete an agreement with the
        terminal agency that services
        them.

    1.  Used as a communications tool
        to inform agencies as to system
        rules, regulations, state and
        federal laws concerning use of
        system data.

        a.  NCIC/Control Terminal Agency
            Agreement

        b.  IDACS/Terminal Agency
            Agreement

        c.  Terminal/Non-Terminal Agency
            Agreement

        d.  Control Terminal/Statutory
            Agency Agreement

2. Terminal Agency should document violations of rules and regulations and show that they have been discussed with the offending agency before canceling any agreement.

J. Audits (IDACS Security Inspections)

1. Periodic announced and unannounced inspections are made to identify areas for improvement.

2. Areas inspected include:

   a. compliance with terminal security

   b. compliance with operator certification program

   c. compliance with records keeping rules

   d. compliance with accepted validation procedures

   e. are manuals up-to-date

   f. are newsletters up-to-date

   g. are agreements up-to-date

3. Areas for improvement discussed with the coordinator and/or agency head.

K. Indiana 240 IAC 5-2-12, IDACS Sanctions

   The IDACS Committee shall review Violations of IDACS/NCIC/NLETS Rules and Operational Procedures and make recommendations to the State Police Superintendent to impose Sanctions on user Agencies.

   (A) Objectives of the Sanction Procedure

   (1) Develop and implement, with the State Police Superintendent's approval, a sanction procedure for SYSTEM rules, regulations and procedures violations.

(2) Create an awareness among
user agencies of the importance
of following rules, regulations,
and procedures in order to
minimize the risk to liabilities
that may be incurred by misuse of
the SYSTEM and its data.

(B) Sanction Requirements

(1) Shall be in accordance with
current NCIC/NLETS Sanction
guidelines.

(2) Require the User Agency Head
to reply within 30 days of the
receipt of a notice of violation
or probation as to the steps
being taken to correct the
situation.

(3) Create sanction procedures
that include: verbal and written
warnings, written notices of
violation, written notices of
probation, temporary and
permanent suspension of service.

(4) Temporary or permanent
suspension of service to begin
after the agency head receives
the suspension notice.

2. NCIC Sanctions in place to assist
   Control Terminal Agency in enforcement
   of system regulations.

L. Risk Analysis Survey for the Wanted
   Person File

   Risk in the Wanted Person File
   results from procedures that expose
   the agency to civil suit due to the
   lack of sufficient care in maintaining
   records. The risk identified is a
   record entered in IDACS/NCIC
   containing inaccurate and incomplete
   information, that is, a record not
   being cleared when appropriate. Either
   risk is significant and may result in
   the arrest of an innocent citizen, the
   failure to arrest a sought-after
   criminal, or the death of an
   unsuspecting officer.

   The following evaluation can help
   identify weaknesses in an agency's

policies.

<u>Instructions For Completing This
Evaluation</u>

For each of the following questions,
select the appropriate answer for your
agency's situation. Circle the
corresponding number. Add the circled
numbers, then compare the total to the
risk level ranges listed after the last
question.

1.  Documentation of Entry Procedures.

    a.  Written procedure and checklist   1
    b.  Written procedure or checklist    2
    C.  Well-defined oral procedures      5
    d.  No well-defined procedures       10

2.  Type of warrants entered.

    a.  Felony only                       1
    b.  Felony and serious misdemeanors   3
    c.  All warrants                     10

3.  Extradition review

    a.  Formal review of extradition
        by appropriate authority,
        confirmed in writing             1
    b.  Formal review, but not
        confirmed in writing             2
    C.  Informal review                  4
    d.  No extradition review           10

4.  Basis for entry

    a.  Entry made using original
        warrant                          1
    b.  Entry made using copy of
        warrant, with established
        control to ensure notification
        if dismissed                     2
    c.  Entry made using copy of
        warrant, no controls             5
    d.  Entry by written request, no
        warrant                          7
    e.  Entry by oral request, no
        warrant                         10

5.  Quality control procedures

    a.  criminal history records
        checked, entry checked by
        third person, entry message
        filed                            1

```
b.  Criminal history records
    checked, entry checked by
    third person                   2
c.  Entry checked by third
    person, entry message filed    4
d.  Criminal history records
    checked, entry message filed   5
e.  Entry checked by third person  6
f.  Criminal history records
    checked                        7
g.  Entry message filed            9
h.  No quality assurance measures 10
```

6.  Validation procedure

```
a.  Total compliance with
    validation definition          1
b.  No compliance with
    validation definition         10
```

7.  Hit  confirmation

```
a.  original warrant verified,
    case report reviewed           1
b.  original warrant verified     3
c.  Case report reviewed          5
d.  Card file or log book
    reviewed                      7
e.  No satisfactory procedures   10
```

If written procedures exist,
subtract one point.

8.  Documentation of procedures for
    clearing entries

```
a.  Written procedure and
    checklist                      1
b.  Written procedure or
    checklist                      2
C.  Well-defined oral procedures   5
d.  No well-defined procedures    10
```

Risk Level

```
LOW RISK       Less than 21 points
MODERATE RISK  21 through 34 points
HIGH RISK      35 or more points
```

Within each of the individual categories,
risk is assessed as follows:

```
1-3  Low Risk
4-7  Moderate Risk- procedures should
     be reviewed and improved where
     possible.
8-10 High Risk- procedures are
```

insufficient must be improved
immediately.

M.  Risk Analysis for the Vehicle File

Risk in the Vehicle File results from
procedures that expose the agency to civil
suit due to the lack of sufficient care in
maintaining records. The risk identified
is a record entered in IDACS/NCIC
containing inaccurate and incomplete
information, that is, information that
will result in an erroneous hit or will
prevent a proper hit from occurring. It
is also defined as the record not being
cleared when appropriate. Either risk is
significant and may result in the arrest
of an innocent citizen, the failure to
arrest a sought-after criminal, or the
death of an unsuspecting officer.

The following evaluation can help
identify weaknesses in an agency's
policies.

<u>Instructions For Completing This
Evaluation</u>

For each of the following questions,
select the appropriate answer for your
agency's situation. circle the
corresponding number.  Add the circled
numbers, then compare the total to the
risk level ranges listed after the last
question.

1.  Documentation of Entry Procedures.

    a.  Written procedure and checklist      1
    b.  Written procedure or checklist        2
    C.  Well-defined oral procedures          5
    d.  No well-defined procedures           10

2.  Basis for entry

    a.  Officers report (written or oral),
        complainants written
        acknowledgement required.            1
    b.  officers report (written or oral)    2
    c.  Oral report by complainant,
        follow up by officer within
        12 hours                             6
    d.  Oral report by complainant,
        no follow up                        10

3.  Quality control procedures

      a.  BMV checked, entry checked by
         third person, entry message
         filed                         1
      b.  BMV checked, entry checked by a
         third person                2
      c.  Entry checked by a third person,
         entry message filed        4
      d.  BMV checked, entry message filed   5
      e.  Entry checked by a third person   6
      f.  BMV checked                     7
      g.  Entry message filed             9
      h.  No quality assurance measures    10

   4.  Validation procedure

      a.  Total compliance with validation
         definition                     1
      b.  No compliance with validation
         definition                    10

   5.  Hit confirmation

      a.  Case report used for hit
         confirmation                   1
      b.  Log book or card file used for
         hit confirmation            8
      c.  No satisfactory procedures      10

   6.  Documentation of procedures for
      clearing entries

      a.  Written procedure and checklist   1
      b.  Written procedure or checklist    2
      c.  Well-defined oral procedures     5
      d.  No well-defined procedures      10

Risk Level

LOW RISK              Less than 13 points
MODERATE RISK 13 through 28 points
HIGH RISK           28 or more points

Within each of the individual categories,
risk is assessed as follows:

1-3  Low Risk
4-7  Moderate Risk- procedures should be
     reviewed and improved where possible.
8-10 High Risk- procedures are insufficient
     and must be improved immediately.

-----------------------------------------------

V.   Summary

   A.  Suggested Additional Reading

1.   [Part I, IDACS Manual](#)

2.   Intro  Section, NCIC Manual

3.   Section 10 (111), NCIC Manual

4.   NCIC Publications

     a.   The investigative tool

     b.   NCIC Off-Line Search

     C.   Extradition of Wanted Persons

     d.   Areas of Liability

5.   Federal Title 28

     a.   As it relates to use of
          criminal history.

B.   IDACS/NCIC importance to law
     enforcement/ criminal justice.

     1.   All of our efforts are needed to
          continue to keep the system a
          viable and efficient law
          enforcement tool.

C.   Importance of Liabilities

     1.   It is important for criminal justice
          administrators to understand the
          civil liabilities that could be
          incurred for mishandling of system
          data.

     2.   Following system rules, regulations,
          procedures could reduce the risk of
          liabilities.